REMARKS

Claims 19, 22, 48 and 51 have been cancelled. Claims 1-7, 9-18, 20, 21, 23-37, 39-41, 44-47, 49, 50, 52-54 are still pending in this application.

The independent claims 1, 25, 37 and 52 had been rejected under 35 USC §103 as being unpatentable over *Carrott et al.* (*Carrott*) in view of *Tsuei et al.* (*Tsuei*).

Each independent claim requires an enrollment process in which a trusted party verifies the <u>identity</u> of the presenter using the enrollment data and then associates authentication data (for example, a password) with the presenter. The trusted party also communicates the password to the presenter (or vice versa); the password is secret in that it is known only to the trusted party and to the presenter.

The advantage of the enrollment process is that the trusted party authenticates the presenter and the associated profile data such that the trusted party can later authenticate that any profile data submitted by the presenter to a merchant (an "acceptor") during a later transaction is authentic. The password established during the enrollment process is later used by the presenter to prove that he is who he says he is.

Claim 1

Claim 1 now requires:

<u>communicating said authentication data between said trusted party and said presenter during said enrollment process, said authentication data being known only to said trusted party and to said presenter.</u>

The advantage is that once the trusted party has verified the identity of the presenter during the enrollment process, authentication data (such as a password) is shared between the trusted party and the presenter, and the presenter can later use this password to prove who he says he is.

Applicant acknowledges the first paragraph of page 3 of the final office action in which the Examiner present arguments as to why *Tsuei* discloses verifying the identity of the applicant during an enrollment process. Respectfully, Applicant points out how these citations to *Tsuei* differ from the claimed invention.

Tsuei discloses a central database repository that holds customer information; the database is used to compare this information against third-party requests and thus verify the accuracy of the third-party requests. But, if the customer information in the central database is not correct to begin with, there can be no authentication.

Paragraph 14 of *Tsuei* is referring to authenticating customer information for an information requester by the central database repository. In other words, the central database holds customer information (which it believes is authentic) and is authenticating that information for a third party who is asking for it. The customer information is already in the central database. If it was false information to begin with, the central database will merely be authenticating false information. There is no discussion of verifying the identity of the customer himself when the customer supplies this information during an enrollment process so that this information can become part of the central database.

Paragraph 17 discusses the same system referred to in paragraph 14. Reference to "the true identity of an individual subscriber" simply refers to the existence in the central database of customer information for a particular subscriber. As mentioned above, there is no guarantee that this customer information identifies a particular subscriber because the customer's identity is not verified when he supplies this information in the first place to the central database.

Paragraph 19 discloses that a subscriber profile includes physical address, Social Security number, etc. Applicant does not dispute that a customer provides this information as part of a traditional credit card application process (see *Tsuei* beginning at paragraph 90 and Reply mailed October 10, 2005); the point is that the trusted party does not take this information during the enrollment process and verify the actual identity of the customer. The information is accepted at face value.

Paragraph 66 discloses a process similar to the above paragraphs. The central database looks up information on a particular cardholder in response to a request from a third party. Assuming that the central database information is valid, the database can authenticate third-party requests. But, what is missing is verification of the identity of the customer when this customer information is first submitted to the central database during an enrollment process. If the customer information is not verified when submitted by the customer, then it is entirely possible that the customer information is false.

Claim 25, 37 and 52 also requires an enrollment process in which the trusted party verifies the identity of the presenter, and it is also submitted that these elements are not taught or suggested by *Tsuei*.
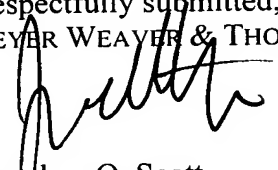
Disclosure of Related Applications

The following pending applications are related to the instant application: 09/842,313; 10/384,735; 10/270,149; 10/156,271 and 10/838,719. It is believed that Office actions in these related applications will contain arguments relevant to the instant application, and Applicant requests that the Examiner review all of the Office actions from these related applications.

Regarding the comments in the final Office action, Applicant would like to point out that what is being disclosed are the above-related *Office actions* not Applicant's *replies* to those Office actions. These Office actions are being disclosed not because Applicant believes these actions will necessarily support Applicant's position, but because they are relevant to the claimed subject matter and might possibly support the Examiner's position.

Consideration of this application and issuance of a Notice of Allowance at an early date are respectfully requested. If the Examiner believes a telephone conference would in any way expedite prosecution, please do not hesitate to telephone the undersigned at (612) 252-3330.

Respectfully submitted,
BEYER WEAVER & THOMAS

Jonathan O. Scott
Registration No. 39,364

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778

Telephone: (612) 252-3330
Facsimile: (612) 825-6304